Business & Economic Review: Vol. 10, No.2 2018 pp. 55-64
DOI: dx.doi.org/10.22547/BER/10.2.3

When 'Ameen' Turns into a Thief: A Case of Weak Internal Controls in a Commercial Bank

Ali Abdullah[1], Shafiullah Jan[2], Adnan Malik[3]

Abstract

This study gives an overview of different operational activities taking place at a bank's branch at any given time. Along with the activities, it also highlights the weaknesses underlying in the system being followed. It gives us the idea of how things could turnaround when an "Ameen turned into a thief". The study discusses the glitches related to Know Your Customer (KYC) policies, staff transfers, password sharing, issuance requests and delivery of chequebooks and debit cards, undelivered statements of accounts and letter of thanks. This study also describes how people can misuse their being a member of a particular gender or class and the respect and attention they enjoy due to the associated cultural values and norms; in a negative manner and take undue advantage of it. This study revolves around the issuance of debit card in one of the accounts and a chequebook in another account and how they were misused to make unauthorized withdrawals from the accounts. The roles of different staff members involved are thoroughly discussed.

1. Introduction

Banking is an important service industry (Ullah, Al-Karaghouli, & Jan, 2017) and it helps in mobilizing the financial resources in any economy. People consider bankers as 'Ameen' of their money and they tend to believe in them. General public brings in their money because there is a strong component of trust associated with the word 'Ameen'. This is the very reason that every action the banker takes on behalf of his customer is always assumed to be taken in 'good faith' until and unless it is proved otherwise. Furthermore, in Islamic doctrine, individuals are bound to be responsibility for whatever they choose, therefore, bankers in the context of Islam are not only responsible to customers for their faith in them but also answerable to Allah on the day of judgement (Jan, Ullah, & Asutay, 2015; Jan, Khan, & Ullah, 2018).

1 *PhD Scholar, Institute of Management Sciences, Peshawar. Email: ali.abdullah@imsciences.edu.pk*
2 *Assistant Professor, Institute of Management Sciences, Peshawar.*
Email: shafiullah.jan@imsciences.edu.pk
3 *PhD Scholar, Institute of Management Sciences, Peshawar. Email: adnan.malik@imsciences.edu.pk*

ARTICLE HISTORY

18 May, 18	Submission Received	30 May, 18 First Review
6 Jun, 18	Second Review	15 Jun, 18 Revised Version of Both Reviews
25 Jun, 18	Accepted	

Due to its imperative nature and involvement of money, especially the money related to public, it becomes very important to monitor and regulate this industry in order to maintain and retain the confidence of the public in the system. To achieve this goal the State Bank of Pakistan, which is the regulatory body of the banking industry in Pakistan, provides guidelines related to the procedures that are to be followed at commercial banks[4]. Alongside, these guidelines provided by the State Bank of Pakistan (SBP), banks do design their own Standard Operating Procedures (SOPs). The Code of Conduct brings out uniformity and standardization in the processes followed in different activities at the bank[5]. In designing and developing these processes audit and regulatory compliance remain the basic driving force. In case of Islamic financial institutions achieving Shariah compliance is also mandatory.

This focused misuse of internal control happened at one of the bank's branches located in Peshawar city. It was a busy branch and mainly had doctors, government employees, hospital staff, gold merchants, and businessmen as their main customers. Primarily, doctors and hospital staff since the branch was situated inside the premises of one of the largest hospitals in Peshawar city. This branch was basically a pooling branch in nature and not doing financing. It had a huge payroll of seasoned doctors, so generating deposits were not a problem at this location. Those doctors didn't make frequent withdrawals, so large amounts of deposits were present in the branch. Along with other services, this branch used to process and disburse the salaries for the whole hospital staff including doctors, paramedical staff, technicians and other employees.

2. Noncompliance with Staff Transfers Policy

Most of the banks operating in Pakistan have a policy that a staff member is not allowed to work in a specific branch for more than 3 years and has to be transferred to another branch so that they may not get involved in personal interactions and relationships with the customers or they may collude with staff. As a result, the staff member may not be able to exploit the weaknesses prevailing in the system, if there are any. Alongside, the transfers there is a concept of mandatory leave in the banking system which allows for the officers to be on leave from office for fifteen consecutive days.

The staff member involved in the fraudulent activity was working at the same branch as a Customer Service Officer (CSO) for the past five consecutive years. She used to be intensively involved in the salary processing phase. She knew all the details of the salary lists and she used to correct all the flaws and mistakes on the list. She knew the account details of the majority of the people. The manager believed upon her replacement, the new CSO would take time to adapt to the environment and

4 *http://www.sbp.org.pk/l_frame/Revised-AML-CFT-Regulations.pdf*
5 *https://www.mcb.com.pk/assets/MCB-cod-em ploye-new.pdf*

unavoidable challenges may arise because of this replacement. Here it is very important to inform that disbursement of salary on the 1st day of every month was very crucial since the hospital's employees would not tolerate any delays in the process and could start agitation. To avoid the chaos, which could arise due to nonpayment of salaries on time, the manager breached the policy of transferring her.

Since she was an employee and had access to the system and furthermore she was a Customer Service Officer who was involved in extensive inquiries related to the customer's accounts, she was well aware of the three key account characteristics needed to conduct a fraud, firstly, the accounts which had huge amount of deposits, secondly, which had easy specimen signatures and thirdly, the account owners who made fewer inquiries to their accounts.

Keeping in view her experience of processing the salaries and keen observations on the above-mentioned factors, for the past five years, she identified two different accounts. In one of the identified account, which belonged to a lady doctor, she successfully applied for a supplementary debit card which had a daily withdrawal limit of Rs. 25,000, which she eventually used for making the unauthorized withdrawals. The second account belonged to a male doctor, who had a very easy to fake specimen signature; she issued an unauthorized chequebook for twenty-five leaves, in addition to already issued chequebook to the customer, and kept it in her own custody for future misuse.

3. Non Maintenance of Customer Secrecy

Maintenance of customer's confidentiality is one of the basic rights of the customer towards the bank. There was a problem with this important factor as well. Doctors who held the major portion of the branch's deposit usually used to send their assistants (trusted contacts) to the bank for the extraction of their account details. The lady CSO in question used to interact with them and provided them with all the details. Even the information was provided on a phone call without verifying the identity of the customer. This may be due to doctor's negligence or maybe their busy routine restricted them to visit branch personally. Yet another reason could be the negligence of the bank or maybe because of the cultural norms of the society where preferential treatment is given to the riches.

Banking business everywhere in the world is unique in nature since every customer of the bank expects a personalized treatment from his banker. The customer thinks that the banker is well aware of his financial resources and he is exposed before his banker. The banker, on the other hand, is doing his job and he tries to provide personal attention to the customers in anticipation of getting more and more business

from them. The banker is always at a back foot in this scenario because he is hungry for additional deposits. Banker always tries to oblige his customers and in doing so he provides more than required respect and favors to them. This factor at times is misinterpreted by the customers and they assign very less value to the self-esteem and self-respect of the banker and they expect everything to be done the way they want it to be.

Here at Peshawar, this culture is more prevalent. If the banker doesn't greet a valued customer, the one with more deposits with the bank, by raising up from his seat for him on his arrival, or doesn't shake his hand or if he doesn't offer the customer a cup of tea, the customer takes this as an insult and would not like it. This culture was very deeply rooted in the bank's branch where this operational lapse happened because most of the account holders were seasoned and experienced doctors with a handsome amount of deposits with the bank and they were very much in the category of valued clients to expect preferential treatment from bankers.

4. Know Your Customer (KYC)

To minimize the risk for financial institutions, the State bank of Pakistan, has provided with prudential regulations[6]. It is not a one-time process rather it is an ongoing process. As per the guidelines provided by KYC the banker should have complete details of the address of the customer. It includes many other factors as well e.g. knowing and verifying the sources of funds in the accounts. To verify the address of the customer, the bank sends a letter of thanks to the customer's designated address, as soon as the account is opened. To have the chequebook for the new account the customer has to bring in that letter of thanks to the branch which verifies the customer's physical address. Afterward, as the relationship continues, the banks send in periodic statements of accounts to their customers. Account activity for the period January-June is sent in the month of July whereas account activity from July-December is sent in the month of January, in the subsequent year. Undelivered statements of accounts of the customers are delivered back to the respective branch by the head office. It then becomes the responsibility of the branch's Operations Manager to dig out the reasons for their non-delivery. Most of the times the reason is incorrect customer's address. This reason is a clear indication of weak implementation of KYC procedures.

The status of undelivered statements of customer's accounts was worse in the focused branch. The said branch had hundreds of undelivered statements of customer's accounts in their custody and nobody/ responsible officer tried to update the

6 *http://www.sbp.org.pk/bsd/2004/Anex-C7.pdf (Know Your Customer/Customer Due Diligence (KYC/CDD) referred to as regulation 1)*

customer's addresses. Surprisingly, when the fraud was surfaced the first question asked by the inquiry team was related to the delivery of statements of accounts to the customer's address.

5. Issuance Request/Delivery of Chequebooks and Debit Cards

Chequebook and debit cards are safe custody items. They are to be placed under the dual control of two officers. Chequebook issuance requires a requisition duly signed by the Account Holder. The signatures are then verified by the Signature Verification Officer and eventually, Operation Manager authorizes the issuance. The chequebook then arrives at the branch in 3 to 4 working days which needs to be collected by the Account Holder within 90 days. This is the procedure for issuance of computerized printed chequebooks. Branches may also be issued stock of cheque books which do not have printed details on the leaves rather they are standardized leaves with only bank name and logo printed on it. As soon as the branch receives them branch stamp is affixed on each leaf of all the stock received.

Similar is the case with debit cards. It requires a requisition from the account holder requesting the card. The signatures are verified by the Signature Verification Officer. CSO then inputs all the requested details in the software system using his/her own login User ID and password. The Operation Manager then verifies the details punched by the CSO and then further authorizes the requisition for the issuance of the card using his own login User ID and password. The card then arrives at the branch which needs to be collected by the customer or is delivered to the designated address of the customer. The card then needs to be activated by the calling the helpline and generating the desired pin code by the customer himself using the designated telephone numbers or the branch's telephone numbers.

Some major flaws happened in this process. The CSO asked an intern working at the branch to fill in the debit card and chequebook requisitions for the customers she had already shortlisted using her research for the intended fraud. Not knowing the hazards of it, the intern filled them up without any suspicion.

As she knew about the customer's specific signature style; on the signature part, to avoid being detected in the writing sample test, she signed the forms by herself; moreover, she used her charm and good friendly relationship with the bank's Signature Verification Officer and managed to verify the signatures as well. Using her own login User ID and password she punched in the required details and then also verified the details and authorized the issuance of debit cards using the Operation Manager's login User ID and password. In this episode, there seems to be another gross irregularity. The Manager Operations had shared his User ID and password

for all sorts of verifications and authentications with all the staff members, perhaps to lessen his workload by delegating the authority. This seemed to pave and eased the way for the fraudulent activity. Had this password not been shared with the staff members the process would have stopped at this point.

Further to the above process, the debit card arrived at the branch. Next step was to collect and activate it. The debit cards and chequebook, and as per rules these are safe custody items, needs to be under lock and key and under dual control of the bank officers. Here yet another gross irregularity was witnessed. The chequebooks and debit cards were lying open in a box outside the strong room and furthermore, they were not under dual control. The registers, which were used to record the acknowledgment of the receipt of debit cards and chequebooks were also lying open in the branch. She easily picked the debit card and a chequebook and made the acknowledgment in the registers since signatures were easy enough for her to forge. She activated the card by calling the helpline from the branch's telephone number and providing all the details required for verification. She could easily provide the verification details because she was an employee herself and she had every access to the system and all the possible information related to verification of the customer as well as the customer profile. Yet another point to be noticed here is, she cleverly selected the account of a lady for this purpose as there is no mechanism, currently in use except for the forensic inquiries, which verifies the sound of the customer.

6. Signatures Acceptance

Here another weakness is highlighted which relates to the time of account opening. Usually, signatures should represent the identity of a person and they should be done in such a manner that there is the minimal possibility of faking them. Here we see that bank, at the time of account opening, seriously ignored this factor and accepted such specimen signatures which were easily faked and copied and created this whole scenario.

If proper procedure was followed at the time of account opening the situation could have been completely avoided. Proper procedure over here could have been not to accept the customer's signature at the time of account opening and suggestion was made to them to create such a signature which is difficult enough to be faked or copied and truly reflects their identity. If this was not possible then the customer should have been suggested to open a photo account where the verifications are not done through signatures rather personal presence of the customer before the authorized officer is mandatory to make any transaction in the account except for making any deposits in the account.

7. The Mystery Cycle

To this point, the field was all set. The card was activated and she along with other accomplices other than from the bank, started making withdrawals of Rs. 25,000 daily using different Automated Teller Machines. SMS alerts for the transactions were not available in those days. Multiple ATM withdrawals were made to the extent that the account reached its limit and was emptied.

Then the next intelligent move she made was that she utilized cheque leaves from the fraudulently issued chequebook she had from the second account. She deposited two cheques, amounting to Rs. 5,65,000 and Rs. 2,25,000 within a time span of 3 days, into the Lady Doctor's account for which she already had the debit card and again started making withdrawals from the account. The specimen signatures for the second account, for which she wrote the 2 cheques, were easy enough to be forged and easily got verified at the bank. The other officer authorized to make the internal transfer at the branch, which transferred these cheques to the lady doctor's account, had a transaction limit of only Rs. 100,000 but he too made use of the shared passwords of the Operation Manager to authorize the transactions.

The lady fraudster and her allies successfully managed to withdraw an amount of Rs. 2.70 Million until the date when the lady doctor herself, for whom the supplementary debit card was issued; came to visit the bank with a query related to all these suspicious withdrawals from her account.

8. Issues Related to ATM Machine

As per standard operations, the ATM machine takes snaps of the individual using the machine at least two or three times, depending on the type of machine in use. As soon as the news broke, the branch officials were confident to get the snaps and CCTV footage data from the machines used for withdrawals. When the request was made to vendors about retrieval of the data for the dates of cash withdrawals, it was disclosed that majority of the cameras installed at the ATM machines were not working all the time and very little amount of data was made available. When the available data was scrutinized it was revealed that the fraudsters had taken this factor into account as well and in all the available snaps and videos the person making withdrawals had covered their face either by using a helmet or a piece of cloth. This reveals their degree of preparation to deal with such incidences.

9. The Aftermath

When the news of this fraud surfaced the incident was immediately reported to the higher authorities and the inquiry team visited the branch the very same day

in order to make the initial inquiry report and gather the evidence. The customers whose accounts were used were called and informed about the mishap. At that time since the problem had just surfaced, the customers too were not excluded from the suspicion and their involvement in the whole process. But later on upon unfolding of the verity, both the customers were excluded from the investigation. The customers were compensated and their account balances were rectified within three weeks of the occurrence. Customers were quickly compensated in order to avoid any reputational loss.

The staff including; Branch Manager, Operations Manager, Signature Verifications Officer and the General Banking Officer who were involved in transferring the cheques were served with the charge sheet and an inquiry committee was formed at the bank level. The CSO's employer was also informed since she was a third party contractual employee.

Furthermore, the bank filed the case in the banking court and fraud was reported to Federal Investigation Agency's (FIA) Financial Crime Division. A deep-rooted inquiry was done by them which took almost a year to conclude which proved the CSO to be guilty of the fraud.

The bank's own inquiry committee recorded the responses of the staff involved. Penalties and certain recommendations were made. The Branch Manager and Operations Manager were transferred to other branches and their bonuses and increments were ceased for the current year and for the next two years. The other two officers were served with a severe warning letter and directed to be careful in the future of any such negligence.

A policy change was also made after the dust settled. Any official found reportedly sharing passwords with others was subjected to direct dismissal from the bank's services. A comprehensive inspection of ATM's cameras and their data backup was made through the machine vendors.

References

Jan, S., Khan, Z., & Ullah, K. (2018). Reflecting on Islamic development process and Sen's capabilities approach. *Absysn Journal of Social Sciences, 11*(1) (forthcoming) 37-48.

Jan, S., Ullah, K., & Asutay, M. (2015). Knowledge, work, and social welfare as Islamic socioeconomic development goals. *Journal of Islamic Banking and Finance, 32*(3), 9-19.

Ullah, K., Al-Karaghouli, W., & Jan, S. (2017). Collaborative Islamic banking service: The case of Ijarah. *Business & Economic Review, 9*(2), 187-202.

Additional Readings

Ullah, K., & Al-Karaghouli, W. (2017). *Understanding Islamic financial services: Theory and practice*. London: KoganPage.

Ayub, M. (2007). *Understanding Islamic finance*. London: John.

Teaching notes

a) Learning objectives

The case is aimed to achieve the following in-class objectives:

- Understand the Standard Operating Procedures involved in some of the important banking operations.
- Understand the significance of minor operating activities, which eventually prove to have a huge impact, if things go wrong.
- Identifying the weaknesses in the role of Branch's Operations Manager.
- Identifying the weaknesses of other staff members of the bank.
- Understanding the importance of following the rules and regulations.

b) Suitability of the case

The case is suitable for:

- Undergraduate and graduate students taking courses in banking laws and regulations
- To be used as a training material for bank's trainees.
- Developing an idea of the banking environment for the students planning an internship at any bank.
- This case can be easily discussed in a class of 90 minutes. 40 minutes for reading the case and 50 minutes for discussion.

c) Assignment questions

- Identify the need for mandatory leave at Banks?
- Why is a letter of thanks sent by the bank to the customer's address?

- What could be the reason behind asking the very first question about the delivery of the statement of account at the first visit of the inspection team?
- What information does the call center use to verify the identity of the customer?